Privacy and Security Tiger Team
Draft Transcript
February 25, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning, everybody, and welcome to the Privacy and Security Tiger Team. This is a Federal Advisory Committee, so there will be opportunity at the end of the call for the public to make comment. The call will go from 10:00 a.m. until about noon.

Let me do a quick roll call of the members. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Egerman?

Paul Egerman – Software Entrepreneur
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Gayle Harrell? Carol Diamond? Judy Faulkner? David McCallie? Neil Calman? David Lansky? Dixie Baker? Micky Tripathi? Rachel Block? Alice Brown?

Alice Brown – National Partnership for Women & Families – Director HITP
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Houston? Wes Rishel? Leslie Francis? Lisa Tutterow?

Lisa Tutterow – Office of the National Coordinator – popHealth Principal
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Adam Greene? Joy Pritts? Did I leave anyone off? Okay, short membership. Paul and Deven, go ahead.

Paul Egerman – Software Entrepreneur
Good morning. This is a little bit of a shortened membership, but it's not a surprise, I suppose. Not only is it Friday morning, it's Friday morning after the HIMSS Conference, where I suspect some people are still proceeding home, or perhaps because the conference is in Florida extended their stay for a few days. Although I am starting to get some e-mails, I don't know if you're getting this, Judy, that some people are having trouble with the phone number working.

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes.

Paul Egerman – Software Entrepreneur

I've got e-mails from Wes—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I had to try for the last ten minutes and I just got through. So I think they're resolving the issue.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay.

Paul Egerman – Software Entrepreneur
Yes, so the e-mail I got from Wes was, "All circuits busy; will keep trying," and an e-mail from Judy Faulkner saying, "Phone number does work, just get busy signal."

Judy Sparrow – Office of the National Coordinator – Executive Director
Alan, can you check into that, please?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I got the all circuits busy—

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I got that same thing. Actually, the last conference call we had I had a similar problem, "All circuits are busy."

Judy Sparrow – Office of the National Coordinator – Executive Director
Let's hope everyone gets in and then I'll take it up with the contractor after the call.

Paul Egerman – Software Entrepreneur
Yes. I'm doing my best to quickly respond—

Deven McGraw – Center for Democracy & Technology – Director
Yes, me too.

Paul Egerman – Software Entrepreneur
—to Wes and—

Judy Sparrow – Office of the National Coordinator – Executive Director
Dixie's on now. Carol's on. Judy Faulkner.

Paul Egerman – Software Entrepreneur
Is Judy on, Judy Faulkner?

Judy Sparrow – Office of the National Coordinator – Executive Director
No, maybe I misspoke, sorry.

Deven McGraw – Center for Democracy & Technology – Director
Yes, she's not on. She's trying to get on. I think we should wait a couple of minutes.

Paul Egerman – Software Entrepreneur
Yes, I'm going to—

Judy Faulkner – Epic Systems – Founder

The number that's on the invitation doesn't work. The number that's in the screen show does. So if people are listening, look at the number on the screen show and then dial that one.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But that's for public comment. The other one works.

Judy Faulkner – Epic Systems – Founder
No—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, it doesn't, I got—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I got—

Judy Faulkner – Epic Systems – Founder
Yes, but I got in.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
—after several failures I was able to get in on the number on the invitation.

Judy Sparrow – Office of the National Coordinator – Executive Director
So the number's 1-877—

Paul Egerman – Software Entrepreneur
Wait, we're on a public call right now, so we don't want the public calling in on the other number, I think.

Judy Faulkner – Epic Systems – Founder
I called in on the other number, and they asked me.

Paul Egerman – Software Entrepreneur
They put you through? Okay.

Judy Faulkner – Epic Systems – Founder
Yes, they did.

Deven McGraw – Center for Democracy & Technology – Director
Okay, good.

Paul Egerman – Software Entrepreneur
Whatever works. What we're going to do here is wait another minute or two to give people a chance, because I have a feeling there might be a few other people who are getting frustrated. But I just want to say it's great to have everybody on the call. So I'm trying to think of what I'm supposed to do to kill a couple of minutes here.

Deven McGraw – Center for Democracy & Technology – Director
I can say something, Paul.

Paul Egerman – Software Entrepreneur
Okay, go ahead, Deven. That would be great.

Deven McGraw – Center for Democracy & Technology – Director
Recall that a couple of calls ago we had distributed a draft of our recommendations put in the format of a framework document mapped to the nationwide data sharing principles and asked for feedback from all of you for gaps and priorities for upcoming meetings. I haven't heard from any of you yet, so don't forget about this, we'll re-circulate it after this call. But the other thing that we are going to do is to post some questions on the blog to get some feedback from the public about policy areas that we have not yet delved into that are going to be critical in terms of fleshing out policies for the Nationwide Health Information Network and/or meaningful use privacy and security criteria, whatever is the particular policy lever we still have to come up with the substance. So Paul and I had a discussion before the call, and this was actually an idea that got generated at one of the sessions that I participated in at HIMSS that we would seek some public comment on this, input from the public about issues to be resolved in the very near future. So stay tuned. We'll try to get that up next week, if I can.

Judy, is there any obstacle to—?

Judy Sparrow – Office of the National Coordinator – Executive Director
No, just let's talk about what you put up and we'll get it up.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

W
Deven, if you could re-circulate, that would be great. But the one other thing I would ask is, and I don't know if this should be prioritized into that or fostered into that prioritization rather, is any pending input that ONC needs either because of HITECH requirements from a regulatory standpoint or other agency requirements from a regulatory standpoint. I don't know the status of disclosures, breach, audit and I'm just wondering if there's a prioritized list of issues from an input standpoint that's needed by the agencies also.

Deven McGraw – Center for Democracy & Technology – Director
That's right. Just as an example, we know that the accounting of disclosure rule changes that were enacted in HITECH but for which there needs to be significant regulatory guidance to implement, that rule just went to OMB two weeks ago. At any rate, it's a really good point. That was just one example.

Paul Egerman – Software Entrepreneur
That's a good point. It' s just about ten past. Do you want to go ahead and re-start now?

Deven McGraw – Center for Democracy & Technology – Director
Yes, let's go ahead.

Paul Egerman – Software Entrepreneur
We'll start over, so this is like a do-over. I'll just say good morning and welcome to our Privacy and Security Tiger Team. What the tiger team is, is a group of individuals who address various security and privacy issues and make recommendations both to the HIT Policy Committee and the HIT Standards Committee. The issue that we are addressing right now, and what you can see on your screen, is an issue that we call "authentication of users."

Just to make sure everybody is synchronized, originally when we got started people were talking about this as provider authentication, I think they meant provider individuals, but we thought it better to rename the topic as "users" for two reasons. One is there's a little ambiguity when you use the word "provider" in terms of who you really mean. But the concept is there are other people, other than clinicians, who use the EHR system and so this is we thought a better way to provide the scope. So the users are people who gain access to an EHR across a network such as the Internet, possibly using mobile devices, so that includes mobile devices. The scope, at least right now, although it's a topic that we will discuss later, is it does not apply to users internal to an enterprise, but again we'll be talking about that a little bit more later. That's the objective of the discussion. Then I think Deven is going to take us through a little bit of the background of what we've done so far, because I think a few people might have missed the last meeting.

Deven McGraw – Center for Democracy & Technology – Director

Yes. Thank you, Paul. Again, this is a continuation of a discussion that we began really actually two calls ago, but spent all of our last call discussing, for those of you who were able to join us. Through most of the call we seemed to reach a bit of a consensus from a policy standpoint that an assurance level of three per the NIST assurance levels, which is a common set of guideposts that certainly are used within government and provides a jumping off point for many private sector initiatives. I certainly heard from, in between the meetings, at least one major private sector initiative, the Kantara Initiative, that has looked at the NIST guidance and come up with some applications for the private sector. But substantively my understanding is it's very similar. So these NIST documents, even though they were intended for use by the federal government, have been widely utilized as a baseline for coming up with private sector policies, so when we say, "level three assurance," what do we really mean by that? Well, it's a high degree of confidence that the claimant in an authentication process, the person who is seeking the information, is actually who they claim to be.

This on slide four is just a reminder of then this comes from the NIST materials, sort of what is a way of landing on the appropriate assurance level, and certainly, the highest level of assurance is four. I think in general in our tiger team discussions we were not terribly comfortable with going any lower than three again as a minimum. It's not as though policies and practices of individual institutions couldn't be higher. But I think we're thinking about from a policy standpoint whether there ought to be a minimum threshold below which no one can go. Because certainly we know that in the HIPAA security rule, it does not necessarily specify levels of assurance.

If you move to, and this is yet another example of how taking the level of assurance, given a certain level of assurance that you were trying to hit, what does that mean in terms of factors for authentication and then there are also in this chart components for identity proofing. You'll see in particular that there's a difference between level two, level three, and level four, there was a difference between all four levels, quite frankly, but level two requires only single factor authentication, which as we'll talk about in a minute is a log-on and password would be single factor. Levels three and four, which I think intrinsically were at the levels of competence that we wanted to reach, require additional factors, more than just a log-on and password in order to authenticate at those levels of assurance.

We talked a little bit at our last meeting about what's required for prescribing of controlled substances under the DEA rule, and they used the NIST document that we just talked about, but they adopted it. But it does, in order to prescribe controlled substances required to factor authentication chosen from really three different options, one of which is the password, which is the knowledge token. But it also requires one other, either a hard token or a biometric, which is acceptable but not required as the second factor. Then there are also stringent identity proofing requirements. Again, to reach level three, if you go strictly by the NIST assurance levels you are going to need a knowledge token, a password would suffice there, but it's not the only thing, as you'll see, that qualifies. But you also need to have a hard token.

One of the things that we talked a little bit about on our last call was whether the computer itself, such as a recognized IP address or some other way that the computer that you're using can be recognized, is that also a factor. So that a password, along with using the laptop that's been registered to you or the PDA that's been registered to you, does that count as the second factor and per the NIST guidance it does not. The computer being used is not by itself a factor. That was a question that came up on our last call and we've got an answer for that now.

Again, we were circling around some comfort level with landing on a minimum level three assurance, and then where we got into a little bit of trouble in terms of closing on some recommendations was, well, are we actually prepared to require multi-factor authentication, which requires at least one of which is a hard token.

Leslie Francis – NCVHS – Co-Chair
Deven, I apologize for being late on the call. I tried to call in and—

Deven McGraw – Center for Democracy & Technology – Director
You weren't the only one, Leslie. Don't worry about it.

Leslie Francis – NCVHS – Co-Chair
I'm here now, but I just want to be sure to clarify, this is authentication for individuals whose original identity has already been established by, for example, the system for whom they work.

Deven McGraw – Center for Democracy & Technology – Director
That's right. We are talking about individual users within a provider or a hospital health plan. We're leaving off to our next set of issues how you identify and authenticate patients.

Leslie Francis – NCVHS – Co-Chair
The question there is not just patients versus employed individuals, but the assumption is that the initial whatever this person gets, a password or whatever, that the entity has taken care of making sure that the individual is who they say they are at the point of initial access.

Deven McGraw – Center for Democracy & Technology – Director
Right, that they have been identity proofed.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, maybe I'm missing misinterpreting Leslie's comment, but this could be applied to, say, a provider logging in to the EHR at the institution where they're practicing, so both of the two factors would be provided at that time. They wouldn't have already logged on to some network within that entity first. They could be coming in from their home or using a mobile device or something like that, right?

Deven McGraw – Center for Democracy & Technology – Director
Right, but I think Leslie's question was to the issue of how do their credentials get issued in the first place.

Leslie Francis – NCVHS – Co-Chair
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Oh, okay. I thought she said they were first authenticated. What you're saying is first credentialed.

Leslie Francis – NCVHS – Co-Chair
Right.

Paul Egerman – Software Entrepreneur
That's correct. The assumption is they already have a user name and password.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Sure.

Leslie Francis – NCVHS – Co-Chair
They've already got the initial set of whatever it is you're going to now use to authenticate them by.

Paul Egerman – Software Entrepreneur
That's right.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Leslie Francis – NCVHS – Co-Chair
Yes, I was just wanting to be sure to clarify that. I agree with you, Dixie, whatever we say here has got to deal with the off-site person, which is one of the reasons why a particular IP address is a problem.

Deven McGraw – Center for Democracy & Technology – Director
Right, because you don't necessarily know who's using the computer.

Paul Egerman – Software Entrepreneur
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, I have a question about your slide that you have up there now. You say the computer being used is not by itself a factor. In other words, it can't be one of the two factors?

Deven McGraw – Center for Democracy & Technology – Director
That's right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So I think we need to think about the wording there, because it sounds like—

Deven McGraw – Center for Democracy & Technology – Director
Okay, I see.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay, thanks.

Paul Egerman – Software Entrepreneur
Dixie, that's a great question and a great clarification. Because one of the reasons we're reviewing this is in a prior call—and I think you were not on the call because you were on the way to D.C. for the hearing—I was leading a discussion and I erroneously said, well, the computer could be one of the factors. That helped reach us to a conclusion that level three was going to work. Then a number of people very correctly said, "Not so fast."

Deven McGraw – Center for Democracy & Technology – Director
I think some of us also are thinking about the online banking that we do and recognize that when we try to log on to our bank accounts from computers that we don't typically use we get prompted with additional knowledge based questions. So the assumption is that there's some identification of the computer that's part of the authentication process and we wondered whether it could be to reach you to level three. But we know that in fact, at least using the NIST guidance as our baseline, that doesn't count.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I asked about this. Gartner's privacy ... is about bank authentication schemes. Their sense is that many of them, such as what's your favorite ice cream, are more flash than value but that most banks are doing various active detection schemes at the same time, such as IP addresses and other things, that are not officially part of the authentication or not visible to the person as part of the authentication process. So they would recommend we go light. I didn't ask them to do the recommendation, but based on their interpretation counting on those things is not a really effective authentication scheme.

Paul Egerman – Software Entrepreneur
That's good comments, Wes. That might lead us to the next slide, although I'm not sure if you're ready to go there yet, Deven.

Deven McGraw – Center for Democracy & Technology – Director
Yes, I think so. I just want to make sure that I had accurately presented the material on the slide, so I wanted to pause for a minute for the MITRE folks, who have really helped us prepare for this set of calls on this topic, and make sure that there wasn't anything that I left out or that I misspoke.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Deven, I just want to check on the last bullet, the biometrics. Can you explain what that bullet really means?

Deven McGraw – Center for Democracy & Technology – Director
That's actually a good question. Jay, can you help out on that one?

Jay Brennan – MITRE
Yes, there are a couple of things here that might be clarified. That one is, for instance, in the DEA, as I understand it—I'm no expert, I think Dixie is actually an expert on this—the DEA when they adapted … allowed a person to take a biometric image of, say, a finger and then store that on a computer. Then the other side of the authentication would have the same thing. At the time of authentication they would present this, I guess, file and it would be matched up against the one on the other side. Now, NIST doesn't think that's a factor of authentication. But it does allow biometrics when you actually open up some other device with the biometrics. The example would be I have a cryptographic card and it by itself has a little fingerprint reader on it, so in order to enable the card I stick my finger in the fingerprint reader and that activates the card and then I use the card immediately to go through an authentication protocol. NIST considers that two factor authentication, even though biometrics was used. The biometric is being used to activate some other device. Does that explain it?

Deven McGraw – Center for Democracy & Technology – Director
Yes, it's very complicated, though.

Jay Brennan – MITRE
Yes, well I mean—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't understand it. I do know that biometrics are pretty powerful these days, but you don't really capture the image, you don't really ever send the image over the wire.

Deven McGraw – Center for Democracy & Technology – Director
Right. That's also a distinction between what's in 863 and what the DEA came up with, because I'm just going to go back one slide for a second, in the two factor authentication for the DEA rule a biometric is one possible factor. So in other words, they didn't follow the NIST guidance to a T, they modified it a little bit. But it is two factor authentication and you choose two from this list of three categories.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I wasn't aware that biometrics couldn't be the second factor. That's interesting.

Paul Egerman – Software Entrepreneur
I just want to be clear, so biometrics is not a second factor except for this interesting exception that's listed below?

Jay Brennan – MITRE
That's right.

Deven McGraw – Center for Democracy & Technology – Director
Not in this 863. It is for DEA.

Jay Brennan – MITRE
We have another slide in there that lists all the factors that NIST has, in the 863 draft anyway, and biometrics is not on that list. But they do allow biometrics to be used and they count as two factor authentication, in the case I just went through, that is, when a biometric is used to activate some other device.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Do we know the rationale for why NIST does not provide for biometric—?

Jay Brennan – MITRE
I'm afraid you're going to have to ask NIST for that. I don't know the rationale.

Paul Egerman – Software Entrepreneur
Has anybody had experience using biometrics on this call? I'm just curious.

Deven McGraw – Center for Democracy & Technology – Director
We might have somebody on the public.

Leslie Francis – NCVHS – Co-Chair
I do.

W
Yes, I do.

Leslie Francis – NCVHS – Co-Chair
The sports club that I go to has both a biometric and a password.

Judy Faulkner – Epic Systems – Founder
The place I go you put your hand in and they do a palm print. But I just asked somebody here to find whoever in their company figures out the different biometrics that our various customers use so we can get that person on too.

W
Thank you, Judy.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
They certainly were shown at HIMSS quite a bit, biometric devices including fingerprints.

Deven McGraw – Center for Democracy & Technology – Director
Keep in mind, again, we have the NIST guidance, we already said as a tiger team we're not interested in necessarily making something up from scratch, but we also have what the DEA did and they didn't adhere strictly to the NIST guidance, but used it, they've got it. So they treat biometrics slightly differently, but I don't know that we necessarily, it will be helpful to have answers to these questions but I don't know if we necessarily need to come to resolution on biometrics in order to come to at least some overarching policy recommendations.

Paul Egerman – Software Entrepreneur
That's right.

Judy Faulkner – Epic Systems – Founder
One of the things with biometrics that we see is not that you put your fingerprint in and it figures out who you are. In fact, at HIMSS, they had a Harry Potter thing and you did biometrics to open up your storage locker, which I thought was very interesting. But first you say who you are and then they match it to your biometrics to have a much smaller population of comparison.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's how authentication always works.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes.

Judy Faulkner – Epic Systems – Founder
That's why—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That's the concept for the two factors.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Sorry I was late to the call. My experience with fingerprint biometrics is that it's really unreliable in certain people. I'm one of the people that they ... on for some reason.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm another, and it's obvious why I'm not very—

Paul Egerman – Software Entrepreneur
David, that's a good comment because the reason I asked the question, my own personal experience was I tried to use biometrics, so every time I would log on to my computer I tried it myself, and I personally found it annoying because I'd be pushing my finger through five times to get it to work right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – Software Entrepreneur
I didn't know if that was just me, and maybe that's the reason why in the previous slide you have that concept of well, you can somehow initialize a card in effect with biometrics. Because I can see how it works okay if we're going to get into a sports club or something because you just use it only once during the day, well, maybe if you're really athletic twice during the day.

Leslie Francis – NCVHS – Co-Chair
Does anybody have any knowledge of how the iris identification as opposed to hand or finger?

Deven McGraw – Center for Democracy & Technology – Director
I don't. I also think it's an interesting conversation to have, but I think we don't want to base a policy recommendation on anecdotal—

Paul Egerman – Software Entrepreneur
That's correct. David—

Leslie Francis – NCVHS – Co-Chair
—whether we should look at what the evidence is on either of those.

Paul Egerman – Software Entrepreneur
What we really want to do is understand a little bit about what NIST says and then we've really got to get to this straw man recommendation.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
It sounds like we're lacking in two things. One, we're not interested in picking a technology. We're interested in picking a framework that will cover technologies. We have questions about what NIST means that may not be answered right now online. But we need to leave a placeholder there and go on. Assuming that there is a set of recommendations that we can come around, what will we do with it.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Thank you, Wes.

Paul Egerman – Software Entrepreneur
That's a great summary, Wes, so thank you very much. If you look at slide eight, there are two options.

Jay Brennan – MITRE
Paul, can we go back to something on the other slide that I didn't cover and then move on?

Paul Egerman – Software Entrepreneur
Sure. Which slide do you want?

Jay Brennan – MITRE
The one with the knowledge—

Paul Egerman – Software Entrepreneur
Yes.

Jay Brennan – MITRE
A question came up about the use of knowledge, both at NIST and other places, in the financial arena in particular. Now NIST has it in there, but you have to read more than just, well, you can ask the ice cream flavor, which is cute, but what their intent is was to ask enough questions that you essentially get the strength of the password. I think everybody should understand that.

The other thing is in the financial industry many banks are now using what is called risk based authentication, which is not an authentication paradigm that's like the one we're all talking about here. It starts with a different premise, and that is the premise is we should not worry so much about who's at the other end of the line, but what they're about to do. So they gather evidence of whether the transaction that is being proposed is allowable or not, as folks have mentioned, they gather IP addresses, time of day, in some cases you can gather—there are up to 100 factors that banks are looking at.

Now, they don't do this for every transaction, but every time you go to your bank to do an electronic, not every bank, but the modern bank, large banks, every time you go there for a transaction you're being scored for all the factors that they're gathering on you. Typically, what happens, not in all cases, some banks actually use this knowledge piece as an upfront authentication mechanism. My own credit union does that, but typically what happens is you're being scored on this transaction, time of day, amount,

where it's going, IP address, have you been there before, but you have a history of transactions at the bank. If your score doesn't meet what they require typically they will then go into the knowledge question that says, tell me your mother's maiden name or whatever it may be. It's already been pre-registered. If you flunk that then you get the well, call the bank. We're open on Monday. Call the Customer Service desk. That's what's going on there primarily.

Paul Egerman – Software Entrepreneur
Those are very helpful comments in terms of understanding. So one of the basic takeaways I got from your comments was well, the banks are not doing level three or two factor but they're doing other stuff. The other comment I would give is I think we need to be careful sometimes about comparing healthcare to the finance industry, because in a banking transaction if it somehow messes up and the wrong person gains access, well there's a remedy and the remedy is you give back the money. The remedy in healthcare is a little bit harder to figure out. So that's also an important concept to understand.

Going on to the next slide, slide eight, with that basic background information, here are two options. One option is the do the DEA approach to all providers, with biometric use permitted as a factor. The second option is closer to what we've been discussing as examples from banking, where we basically start with an approach that's somewhere between level two and level three, so we require multi factors, but we allow the two factors to be something you know. So the way this would work, the example that was given was if you were signing on as an EHR user from your home, when you put in your user name and password it would ask you one of these knowledge based things about your grandfather's middle name or something like that. If you had the correct answer to that, at least in some examples it might put even like a cookie or something on that machine that says you've done this correctly before and then allow you to operate on that computer. So the question is, are there any other options? Or what do people think, do they like option one or option two?

Deven McGraw – Center for Democracy & Technology – Director
Also, just keep in mind that the use case we're considering here is remote access.

Paul Egerman – Software Entrepreneur
Yes, it's remote access and the EHR user could be a physician, it could be an administrative person operating from their home on a laptop or on a computer, but it could also be remote access on a mobile device that perhaps is, in effect, running through the Internet but it's still a mobile device.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So the gist of this would be it's like NIST in that it requires multi-factor, but unlike NIST it's a broader range of choices.

Paul Egerman – Software Entrepreneur
That's correct. Unlike NIST, it would allow you to do what the banking approach is, it will allow you to have a user name and password but also to provide other information that you know. If you were doing this, let me try to give the extreme example. If you were doing this on a PDA, a handheld device, a BlackBerry or an iPhone or a device like that, the very first time you would use it, under option two you'd put in your user name and password and again it would ask you some other question and you would have to answer that question. Then after you answer that question maybe it would somehow register that device or phone number or put a cookie on the device or use some vehicle to do that, so in subsequent uses you would put in a user name and password. So that's one description of option two.

The same process with option number one, where before you could use your user name or password you'd probably have to do some other process, you'd probably have to sign on to some other device. You'd have to, I don't know, do identity proofing. You'd have to somehow give the phone number or some identification for the cellular device, some other computer system would somehow register that or send it some certificate or something, and then you could use the cellular device but you would have some of the process to do that. Or alternatively you could use the cellular device if you had a hard token, if you had one of these little key things that has sequential numbering, that would be another way you could do it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
In other words, use case two is the equivalent to banking.

Paul Egerman – Software Entrepreneur
It's closer to the banking analogy, that's correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think a third option is just level three.

Paul Egerman – Software Entrepreneur
In other words, option one is the DEA approach—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, but ....

Paul Egerman – Software Entrepreneur
—biometrics, so I guess we'll make it 1A and 1B. Option 1B would be level three without alteration.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, right.

Paul Egerman – Software Entrepreneur
That's .... The only difference is the biometrics between the two.

Deven McGraw – Center for Democracy & Technology – Director
Yes, and I think that would be a hard one is to choose between the two without a lot more detail and some more info gathering on the efficacy of biometrics and why NIST made the decision it did not to rely on it, why the DEA made the decision it did to count it as one of the factors.

Just so folks understand, the reason why we divided this up into two options was that there was a suggestion on our last tiger team call—and, Dixie, I thought it was you who made it, but it might not have been, and you might have been just throwing it out as a straw man for discussion. At any rate was to look at the DEA, that the DEA rules are going to apply to a great many providers even though not necessarily for every transaction and so should that not be the baseline that we would seek to achieve for all transactions since entities are going to have to head in that direction anyway. Option two is a little lighter weight. Maybe we actually could have a 2A and a 2B, with 2A being how it's framed and 2B being, okay, well let's begin with the multi-factor and allowing two factors to be in the knowledge category versus one of them being a hard token or biometrics. That we might want to migrate to that over time would be another alternative to option two as it's written.

Paul Egerman – Software Entrepreneur
Here's the way to frame the discussion. The way we see the two options, and maybe some people see other options, but option one would be to use level three of NIST. If you decide on that you could alter that a little bit the way DEA did, so that's how you get to 1A or 1B. Option one is a level three NIST approach. Option two is more similar to banking. It's something between two and three. So that it's more than one factor but it's not quite as stringent as level three of NIST. In effect, I think the discussion is perhaps a classic security discussion and so, Dixie, you've got to tell me if I'm saying this right, so like an issue of balancing security with utility, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's risk.

Paul Egerman – Software Entrepreneur
Risk with utility. That's a very difficult and subjective thing to do is balancing that, which has got to be an issue that you have with all these things.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I would say based on two factors. Number one, the excellent point that Paul just made that we need to be cautious not to compare it with banking because the risk here is way higher than banking, for exactly the reason Paul pointed out. The second factor is what Deven pointed out, and I did in the last meeting I dialed into, is that I think that the DEA requirements should be our floor, probably the starting point simply because a lot of providers, almost every EHR will be involved in ePrescribing, or should be supporting ePrescribing of controlled substances. In my mind I would say for me the two that I would consider is the DEA approach option one and a strict level three.

I was looking up 863, because I wasn't aware that they didn't use, but they say that biometrics do not constitute secrets suitable for use in the conventional remote authentication protocols addressing this document. In the local authentication case where the claimant is observed, in other words in person, and uses the capture device controlled by the verifier, the authentication does not require biometrics to be kept secret. So they're saying if you're there in person using the biometric device that's provided by the entity that's authenticating, it's okay but coming in over the network and not being able to see you and not having control of the biometric device, that's their reasoning.

Paul Egerman – Software Entrepreneur
Okay, so—

Leslie Francis – NCVHS – Co-Chair
I would just add to that the point that was made much earlier, that banks are engaged in ongoing risk assessment, so it isn't just a flat two factor. I'm very much, for the reasons Dixie just gave, in favor of the stronger approach.

Paul Egerman – Software Entrepreneur
Okay. So let me play devil's advocate—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Paul?

Paul Egerman – Software Entrepreneur
I'm sorry. Was that Wes?

Deven McGraw – Center for Democracy & Technology – Director
Yes, that was Wes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I just want to go on record, and I don't know that this is a diversion from this specific discussion, but I don't agree that the risks are much higher. I think that a million dollar transaction may carry more risk than all the damage that can be done to someone's reputation if they're old anyway. But I do think the risks are quantifiable and can be liquefied in financial transactions, and they're not in health data.

Paul Egerman – Software Entrepreneur
Excellent comment.

Leslie Francis – NCVHS – Co-Chair
In banking, they're also variable, so if I'm withdrawing $20 from the ATM, it's a little different than a million dollar transaction.

Paul Egerman – Software Entrepreneur
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

That's a good point. Of course, I disagree with Wes because especially as we get genomic information in EHRs the whole issue of identity, and once you've lost your genomic identity the game's pretty much over. So I definitely think the risk is higher, but the point that Leslie made, for example, my bank doesn't let you do a transfer or an electronic transaction on line for more than $5,000. So they're limiting the risks there and potentially, I guess, EHRs could limit the risks too by saying you can't access HIV information or all of those highly risky areas, genomic information, remotely. That would be roughly the equivalent of what the banks are doing.

Paul Egerman – Software Entrepreneur
Those are good comments again. I wanted to just play a little bit of devil's advocate and look at option two a little bit, because this is a balance between risk and utility. Also behind this, this is what ... was saying, this is going to be. We call this floor, minimum level for people to do later security and also you can do role-based security, so we can say only certain things, only certain people can do this. This is just the floor. This does not necessarily give you access to everything.

As I look at option number two, I said well let's think about people using the system. The physician wants to use the system to just check laboratory results on a handheld device. Or, somebody's doing coverage over the weekend and the patient calls and says they lost their bottle of some medication. It's not a controlled substance, and they need to get a new prescription on a Saturday, so the on call physician, a classic issue, has to look up the information about the prescription and do a new prescription on a Saturday. The issue there is have we made it difficult for that to occur. You think about another situation where you have a physician or nurse who is asked on short notice to come in and do coverage in an emergency department, I guess if it's an internal user it wouldn't matter. But I just want to say does doing option one reduce the utility of the system to the point where it's just really annoying for these people.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I would agree with Paul on that. I think even the DEA restricts the higher level of authentication to the controlled substance prescribing and not to ordinary prescribing. It goes out of its way to make a workflow that's specific to controlled substances.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But we're talking about a higher level of risk. We're not talking about authenticating within an organization. The DEA rule applies within or remote, so we're really talking about a higher risk authentication situation, and as I said, I think option one, with the DEA exception, should be absolutely the floor.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Have we figured out how to define what remote means? If I'm in the hospital lobby and I use the cell phone to find out where my patients are, which is a very common thing, before I go on rounds, is that remote?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I thought about that too. What about if you're within the confines of the hospital but you're using a wireless device where the wireless signals—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, what if your cell phone is using an IP address rather than a cellular? I think that's so slippery.

Paul Egerman – Software Entrepreneur
Those are good questions, but let's—

Deven McGraw – Center for Democracy & Technology – Director
I think we actually said that it wasn't about physically where you were located, but what is the security of the network that you're using.

Paul Egerman – Software Entrepreneur

Yes, the way that we had proposed talking about this, although I agree with David's comment, it gets difficult, is to say, well, if you're inside the enterprise, the enterprise has its own private network and so the terminals are connected directly to a computer. We're saying that's like a different category.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Is the VPN from home, which puts you inside the enterprise network? Is that remote?

Paul Egerman – Software Entrepreneur
Yes, under this definition the answer would be yes, although you would count the way you get into that VPN as your authentication process.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
There would be a lot of people that don't need the DEA level who will be using the EHR. There must be probably four to five times as many users of the EHR as will require DEA level authentication, because only prescribing physicians have to meet that standard, all the nurses and others—

Paul Egerman – Software Entrepreneur
But there are also administrative people who work from home. So an environment I'm familiar with is like an HIM director over the weekend has to deal with the situation where, I don't know, maybe they're short staffed but they have to assign transcription work or coding work or something and they look to see who's available and they say you need to work on this thing. That's still an EHR user because they're accessing at least portions of the record.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, a visiting nurse would be another case where it's almost 100% remote, but they don't do DEA level security.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But a remote nurse would authenticate themselves one time. The remote authentication it just—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
The DEA requires it each time.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Pardon?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Each time you write a controlled substance.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We're not talking about that. We're talking about remote access. So they go into a home, they authenticate themselves so that they can record things while they're in that home, but they don't authenticate themselves every time they input something. They do it one time.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think we're recognizing some degrees of difference in authentication. It's not unusual for hospitals, even with remote users, to recognize the difference between those who can do things that can directly harm the patients, such as enter an order, and those that are looking at information and put a different level of – but that I think still falls into the rubric. Well, I guess not. I was going to say that's out of our scope. I guess the way to say it is if we say we're talking about authentication for remote access we need to either answer the question remote access for what, or give a range of options depending on the potential for imminent patient harm.

Paul Egerman – Software Entrepreneur
Those are great comments, Wes. In effect, I'm listening to this and there are aspects of this that are déjà vu. This is what we dealt with a little bit when we had to deal with some of the interesting issues about

consent and partial and what parts of the medical record are sensitive. There's a sense of on the one hand it's all sensitive and on the other hand I guess there are things that are more sensitive than others and issues that are more sensitive than others. I suppose the analogy in the banking industry is that there's a $20 transaction and there's a $10 million transaction, and so there's big variations.

Judy Faulkner – Epic Systems – Founder
... on re-authentication it may depend on both the customer and the software because the customer may choose or the provider organization may choose that if the system is sitting there that's been authenticated but nothing has been done on it. Maybe the provider is examining the patient or talking with the patient for a certain period of time and it hits a critical spot, it may require re-authentication because of that time lapse.

Paul Egerman – Software Entrepreneur
That's right, Judy. Another way to ground this discussion, if I understand the HIPAA rules correctly, is that healthcare organizations are supposed to do their own risk analysis, and so the risk analysis should determine exactly what you just said, Judy, if people think something is particularly risky or there's some reason they need to do more.

Judy Faulkner – Epic Systems – Founder
Sometimes they do it even if there's been a time lapse, but it depends on what area of the software they're getting into. They may decide we're going to re-authenticate here regardless.

Deven McGraw – Center for Democracy & Technology – Director
Right, absolutely. Judy, Paul and the folks who have just chimed in, I think there's a couple of assumptions that I'm hearing that we're operating under that I think it might be helpful to articulate. One, to make sure that I'm correct about that, and two, because we don't want to try to look to the authentication levels and factors to be the linchpin of security here, because then we have a tendency to overload it with policy because we're expecting it to do the whole job. One is that we do assume that entities are doing risk assessments. They are required to do so. They are required to do so under HIPAA security rule, and they're required to do so for stage one of Meaningful Use in the privacy and security criteria and address deficiencies. So there is that expectation. We're not trying to override that at all. We're just trying to figure out if there ought to be a baseline below which nobody's risk assessment should be allowed to fall.

Leslie Francis – NCVHS – Co-Chair
Deven?

Deven McGraw – Center for Democracy & Technology – Director
Yes. Hang on. If you wouldn't mind, just let me finish a couple of these assumptions and then I'll open it up. The second is that we expect people to actually audit access to records and monitor it, again, so that the security isn't dependent on these authentication protocols. Then I think the third thing is that we are, in terms of the universe of transactions that are of the most immediate concern, I think we're assuming those for stage one, which is an assumption we made in the consent discussion that helped us reach some conclusions. We should not forego the notion that for certain use cases we might actually make policy recommendations that go above and beyond the baseline. So I'll stop there.

Was that Carol that I heard?

Leslie Francis – NCVHS – Co-Chair
No, it was Leslie. What I want to say is just quickly that the requirement to be doing a risk assessment of the risks and protections in your security practices is not—as I understand it, I might be corrected on this—the same thing as the way when you go to the bank. The bank figures out the risk of the particular transaction with a whole bunch of factors. So while it's absolutely important to rely on overall risk assessments, the immediate banking analogy still isn't quite right on that point.

Deven McGraw – Center for Democracy & Technology – Director
Well, it's not. But I think that the risk assessment is supposed to contemplate the expected access uses and disclosures of the system on an ongoing basis. But that doesn't necessarily mean it gets varied on a per transaction basis.

Leslie Francis – NCVHS – Co-Chair
Right, and my understanding is that in the banking system it does.

Deven McGraw – Center for Democracy & Technology – Director
Okay.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
First, I also want to say I'm joined by Karen Bryce, who's our Deputy Director of Policies and Programs. On this point, I just want to say option two in particular, one concern I have is looking at authentication and isolation and not looking at things like, one, the strength of the factors. So a really strong password can be pretty effective sometimes, potentially more effective than two rather weak tokens. Then the other issue is authentication, as had been suggested a few times, works with other technologies. So log-in attempts would be one example, that limiting the number of log-in attempts can have a huge effect on whether single factor authentication is effective versus multi-factor.

Paul Egerman – Software Entrepreneur
Adam, those are great comments. My question is, based on those comments what are you suggesting?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
I guess one thing is, option one you've got DEA standard and you've got I guess the other option one now is level three NIST, and those are fairly spelled out in detail. Whereas, option two doesn't really talk about the strength of the factors, so it's hard to really be able to judge option two's effectiveness without having some idea of what's the strength, what these different knowledge element tokens might be.

Paul Egerman – Software Entrepreneur
So would you accept option two if there was some discussion about that? Or are you saying that's all a slippery slope, because then we get ourselves into a lot of complicated stuff?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
I don't want to get into the role of saying option one versus option two is better. But it just seems option two is hard to really make a judgment because especially in the HIPAA security rule we have to look at the smaller providers in addition to the larger ones. There might be multi-factor authentication or even single factor authentication that based on the strength of the factor and other technologies may provide the same level of assurance but maybe at a much lower cost potentially than having to do hard tokens. I'm not advocating one versus the other, just that option two is kind of hard to actually compare without knowing the details.

Paul Egerman – Software Entrepreneur
Let me ask about option one, the NIST approach, and ask about how that would get used with a mobile device.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I tell you that both CMS and VA have adopted this AniCAM—

Paul Egerman – Software Entrepreneur
Yes, I got a demonstration of it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
—where they use the cell phone to send them back a one-time authenticator, which is really cheap. So it certainly is doable. It's not—

Paul Egerman – Software Entrepreneur
Yes. Dixie, at HIMSS I got a demonstration. But rather than mention a particular vendor, could you just spend one minute explaining the basic concept of how it works?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
They authenticate themselves using whatever, this is how I understand it, so if there's an AniCAM person out there, they authenticate themselves using the first factor. Then the system, it works much like a secure ID token, but the system sends them back something similar to that number that the security token generates, a number that they then enter as their second factor and they're off and running. So they don't have to have a device other than a cell phone.

Paul Egerman – Software Entrepreneur
So the way it would work is that, say I'm at my computer and I'm looking right now at my handheld device, the way it would work is I log on to that computer, I identify myself, and it asks me some identification questions. Then I tell it some information about my handheld device. I say this is my handheld phone number or something about my handheld device, and the computer sends the handheld device, in effect, a digital certificate or something. I pick up the handheld device and I enter that digital number from the handheld device to confirm that—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You can enter it into the computer.

Paul Egerman – Software Entrepreneur
Yes.

M
And it typically just sends a number, it's a one-time password number.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, it's just a number. Ideally, wherever you're authenticating, like a hospital, you wouldn't have to tell it your phone number. That's part of the authentication. It looks up what number do I call, what was the number that Paul gave me, calls you back and gives you that number so that that's an additional assurance that it's used.

M
Right, you direct it to your phone number through an out of hand process.

Paul Egerman – Software Entrepreneur
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – Software Entrepreneur
The question is do you think that that kind of process works and that I should be asking or concerned about the utility for handheld devices?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. I think the fact that it's been so broadly adopted shows you that it's workable and people don't think it's overly burdensome. I'd like to make a comment about the risk assessment, two comments. Number one, yes, HIPAA requires a risk assessment, but HIPAA doesn't require more than one risk assessment. The latest HIMSS survey shows that about half of covered entities do annual risk assessments. So that's not something that they really have espoused, and what they really have espoused, I can tell you when we had our public hearing in November of 2009, over and over again we heard people, the testifiers say, tell us what to do and we'll do it.

Deven McGraw – Center for Democracy & Technology – Director
Oh yes, I know.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And I think it's easier, and I think that they would appreciate more of just tell them, here's what you have to do and then do it than us telling them, well, we know that you're doing this risk assessment, because they're not. We know they're not.

Paul Egerman – Software Entrepreneur
I'm just curious to hear from the vendors about the issue of utility, of doing this, the DEA approach. David and Judy, what do you think?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think the DEA worked really hard to balance the need for utility against their obvious need for security, and I think most of us here at Cerner anyway think they did a pretty good job of that. But it is burdensome and it hasn't yet been tried at scale. So I think it makes me nervous, as much as I respect what they did, and I have a lot of respect because it's very thoughtful work, it makes me nervous to imply that we push it out to a much broader range of use cases than it's currently targeted at without further experience. I certainly am sympathetic to Dixie's point that it's a well thought out approach and this is highly sensitive stuff, so why not adopt it. That's a compelling argument. The answer is we just don't know exactly what the cost will be.

Judy Faulkner – Epic Systems – Founder
This is Judy. I've got a couple of people here that work on this and they only caught the last portion of what you folks have been saying because they had to come in from different places on the campus, so they're not as caught up with what was said earlier. But do you guys want to add anything to this?

M
This is John. I'm one of our RVs over here at Epic. I'd have to say that I agree with some of the last things that were said there, that this can be very cumbersome for users. I don't know that this is something that has really been scoped out or really tested out in the large scale scenario. Because even authentication tokens and other means that can be less expensive for organizations to implement can be time consuming and a little difficult for end users to adapt to and really start to get used to in their flows without it being something that becomes a hassle for them. Single, very strong factors, things that we're really competent in can be very speedy, but when you start to have to stack them up, where you start to have to have, I have to put my hand down, I have to plug this in, and then I have to enter a number. If we have too many of those happening in sequence in order for a person to really meet the regulatory requirements it can be very difficult on the users for that. That's one of the things that I see driving a lot of organizational considerations as far as what they purchase or not is how acceptable this is going to be for the end users to have to do on a very frequent basis.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But it's important to note that it's not anything you have to plug in and it's not piling up. It's a second factor that could be entered in the computer. It's not that you have to carry an extra device around necessarily.

Paul Egerman – Software Entrepreneur
One thing also that I'd make as an observation is the analogy to the banking system and finance is also not quite right, because we talk about the finance system. First, we're talking about consumers accessing their own files, but you're also talking about consumers who are making a decision to use the Internet, which basically means that there's probably some fair level of comfort using the Internet and they don't necessarily have to do that. We've got a different situation here with the EHR system, because the users, it's not the public, it's, I'll call them employees, although it doesn't quite work. Staff members perhaps

works a little bit better in terms of these people have some employment relationship with the institution and also they don't necessarily really want to use the computer. In other words, the computer system is something that they have to use as part of their work process. In other words, not quite like an optional transaction, something they have to do as part of their work process.

I don't know if that is helpful or not. I hear everything that Dixie and people are saying, and Adam is saying about the risks, and I look at level one and it makes sense. I'm just worried about the whole issue of utility, especially think about the mobile devices. And I know there's a way to do all this stuff, but there's a lot of very interesting stuff that's going on with these mobile devices and that has me nervous. I really don't know the right solution. I don't want people to think I'm advocating for one or the other. I'm just a little bit nervous about it.

M
Yes, I'd just like to say that a lot of people have been impressed with a product. I don't think we can advocate a policy that uses a specific product. If the product is covered by patents, then we have to consider whether we would be implicitly saying that if we described the process.

Deven McGraw – Center for Democracy & Technology – Director
Yes. I'm hearing some points that we might be able to make in consensus, but I want to make sure I'm correct about this. Are people generally still comfortable with the notion that for remote access, the use case we're trying to talk about, we're not comfortable with just single factor authentication. We want there to be a second factor of some sort, but we don't know what would be appropriate for that second factor. Either we don't set any requirements at all and allow organizations in their risk assessments to determine which are appropriate to which types of transactions, or maybe we ask for some help from Standards to flesh some of this out in some more detail in terms of the factors. I don't know. But it seems like a threshold question is, do we at least think that there are two factors that ought to be involved here, assuming that again where we started this conversation was that we wanted a high degree of confidence in remote access circumstances that the person is who they say they are.

Judy Faulkner – Epic Systems – Founder
I think you have a choice. Either do a single, very powerful biometric factor that you can do, and that does, I think, I'm not quite sure why Dixie said you don't have to carry it around, because you don't just do it once every time. Then you do authenticate yourself, you're going to have to have the palm reader or the fingerprint reader or whatever is powerful enough, so either do that or do two. I like that. But I also do like letting each organization decide, because I think if we prescribe it too much we won't allow the innovation that might allow nifty new things in the future to come up.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Judy, I think there may be a misunderstanding here. The biometric is the part that level three doesn't even require. We're not talking about requiring a biometric at all.

Judy Faulkner – Epic Systems – Founder
I understand that, Dixie. I'm saying that if that is used that could be pretty powerful.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Your comment about carrying around a biometric device reader, we're not talking about, and I totally agree with Deven, we're not talking about any particular second single factor. Deven, I like exactly what you said. I think it's really tough and maybe we ask MITRE to go off and look at what others have recommended as second factors. We have two standards that we can model after, 863 and the DEA regulation, and I think going off on our own and coming up with a list, I don't know how wise that is.

Deven McGraw – Center for Democracy & Technology – Director
We've talked a lot about NIST and the DEA approach, but as I mentioned earlier, there certainly are also private sector initiatives. You have a slide on the high trust—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Yes.

Deven McGraw – Center for Democracy & Technology – Director
—deck, and then I mentioned the Kantara Initiative that a number of healthcare organizations have been involved with. I'm hearing a lot of discomfort with landing on a specific approach, but at the same time we clearly acknowledge the risks here and the desire to ensure that people are taking the remote access identification and authentication transactions seriously.

Judy Faulkner – Epic Systems – Founder
Dixie, I'm not disagreeing with you about that the biometrics, well, let me put it differently. Biometrics don't have to be declared as necessary for that, but I think we should leave the organization the choice that if they want to do that then it could be single factor if it's strong enough.

Paul Egerman – Software Entrepreneur
In listening to all of this, let me make a suggestion as to how to respond. I think a big part of our problem is we're designing for the high risk, the DEA case, and it's hard to figure out all the different use cases in situations. So maybe one way of doing this is to say that we're really not going to say specifically what is required for authentication, we're going to say that the institutions have to do risk analysis. But we are going to say you have to do more than just level two, which we would define as user name and password. You have to do more than just level two. But whether or not you go all the way to level three or even beyond that depends on the circumstances.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
When we say level three, in this regard level three has a set of combined specifications for originally credentialing the user authentication and so forth. In this discussion we're really just talking about the authentication role in the levels column, is that right?

Deven McGraw – Center for Democracy & Technology – Director
I think so, yes.

Paul Egerman – Software Entrepreneur
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think that there's another factor to consider, but it's hard to consider, which is whether a controlled substance prescription will be the killer app that finally gets some PKI infrastructure into place. We've been aware for a long time that we have all of the technology we need to do, quite a number of levels of protection on authentication, but the infrastructure, priming the pump, getting it running, there was never an app that demanded it. Now it appears there is, or there will be in a year or so, and does that impact our assessment of the difficulty of doing any other approach. The short answer is going to be we can't say, we don't know. But I think it leads us towards a set of recommendations that do call for re-examination at the point where there is substantial use of controlled substance prescribing, if we get to that point, I guess.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So you're saying reevaluate after a while, Wes, go cautiously and reevaluate?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think we need a recommendation for now, but we need to recognize that there is the potential for structural change in the industry that makes some solutions more practical than they used to seem, and we ought to keep that in mind. I also think that we need to at least consider two levels. I don't think we can consider all use cases, but we ought to consider one level which is the minimum for access for personally identified health information remotely. Recognize that it may be appropriate for other levels based on potential risks such as the ability to dump all records simultaneously or the ability to enter orders or things like that.

Deven McGraw – Center for Democracy & Technology – Director
Wes, can I ask you for just maybe a more detailed articulation of the higher level recommendation that I thought I heard Paul put on the table.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Sure, if he can repeat it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I liked what Paul said.

Deven McGraw – Center for Democracy & Technology – Director
Yes, with the added component of evaluating the application –

Paul Egerman – Software Entrepreneur
I'm sorry. Let me articulate it a little bit differently. As I said, each organization has to do a risk analysis. The risk analysis has to include the roles of the individual and the types of information that the person has access to, but that as a minimum floor for authentication of user that the use of level two is not acceptable. It has to be greater than level two, something more than a single use of name and password for all users. So that doesn't necessarily say it has to be three, but it just has to be greater than two and there has to be this analysis.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, I'm sensitive to what Dixie mentioned about the testimony in 2009.

Paul Egerman – Software Entrepreneur
Where people were saying tell us what to do.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
The risk is—

Paul Egerman – Software Entrepreneur
Yes, that's true.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
—that you'll invest in a technology, roll it out, and then learn effectively they're the equivalent of case law, I think in the law, where you find through a series of decisions by the HIPAA cops that what you just invested in isn't acceptable. If we could argue that not necessarily level three but more than two, such as, and provide some specific examples of what we had in mind, then I think that at least creates a safe cover.

Paul Egerman – Software Entrepreneur
Yes, so you're saying take my proposal but either provide examples or best practices or say something more so people understand what it means.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes.

Paul Egerman – Software Entrepreneur
And two is to say adequate, what is adequate and under what circumstances.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
A two doctor practice which has remote access over the public Internet to its employees would do this. This is what we envision would be an example of acceptable.

Judy Faulkner – Epic Systems – Founder

Did we discuss at all what the NHIN is doing? The folks here in the room were talking about what NHIN is doing for authentication, so some of the overlap is what you're talking about? Is that relevant or not?

Deven McGraw – Center for Democracy & Technology – Director
When you say "the NHIN" are you talking about NHIN Exchange and NHIN Connect, the ones that involve connections to the federal health architecture?

Paul Egerman – Software Entrepreneur
I think she's talking about NHIN Direct.

Judy Faulkner – Epic Systems – Founder
Which one are you talking about?

M
It's the systems connecting to the AO or the network, the centralized repository.

Paul Egerman – Software Entrepreneur
Are you talking about Arien Malec's project?

Deven McGraw – Center for Democracy & Technology – Director
No, not if they were connecting to a central repository. I'm not sure what initiative you're talking about.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think they're talking about Connect—

Deven McGraw – Center for Democracy & Technology – Director
NHIN Connect?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I wasn't aware there was any user authentication ....

Judy Faulkner – Epic Systems – Founder
Do you want to talk about that?

John Scale – Epic Systems
Yes, there is actually user authentication. They have what they're calling the UZI pass, the universal physician identification card. They're Dutch acronyms, I'm sorry. The system that they have is that all providers or really medical professionals are issued with identification cards that have essentially ... certificates on them, paired with a PIN, a password.

M
Is this a U.S. initiative?

M
This is a Netherlands initiative.

Paul Egerman – Software Entrepreneur
It's another country.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
It's NCVI, right?

Judy Faulkner – Epic Systems – Founder
Is it being discussed to incorporate in the U.S.?

M
It's something that—

Judy Faulkner – Epic Systems – Founder
Yes, but is the NHIN talking about incorporating this in the U.S.? Oh, okay. So this is a Dutch—okay.

Paul Egerman – Software Entrepreneur
It sounds interesting, although the observation that I want to make again is that we're talking about users, not necessarily just clinicians or not necessarily physicians. You could have a lot of administrative people, for example, a CEO of a hospital may not be a physician, but that works at home a lot and accesses all kinds of information, quality information. There's probably all kinds of CFOs, there's a lot of people who have access to a lot of the information.

The proposal that we're putting on the table, there's really two choices here so far. Our one choice is to stick with level three. The second choice I'm putting on the table is to say, with Wes' amendment, is you have to do more than level two. You have to evaluate the situation, and here are some examples.

Deven McGraw – Center for Democracy & Technology – Director
Right, and study how well the DEA approach is working—

Paul Egerman – Software Entrepreneur
Yes, well the main reason I personally am hesitant about the DEA approach is that it appears not to be in widespread use. So I'm nervous about setting a floor in a national standard—

Deven McGraw – Center for Democracy & Technology – Director
No, no, no, but that's not what I'm suggesting. What I thought I heard Wes say was this is going to be required of providers prescribing controlled substances and we ought to do some examination of how it works as it gets rolled out.

Paul Egerman – Software Entrepreneur
That's exactly right. That's actually what I was trying to say is I don't want to set that as a standard until we have some understanding whether or not it's effective in actual use.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That's why I called it the reevaluation—

Paul Egerman – Software Entrepreneur
... more than two but not quite willing to say three yet because I'm just a little bit nervous that maybe it works and maybe it doesn't.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
That's why I called for reevaluation, Paul. But I just want to make clear that we're thinking of a set of use cases that's much broader than prescribing controlled substances. The reason I think it's highly relevant is that if it rolls out successfully and gets adopted it will be the first time that I know of in—well, not the first time, but it will be remarkable in that a widespread, multi-organizational PKI-based scheme gets rolled out that would create a lot of the mechanisms. The businesses in the IT infrastructure that would make things that we currently think are impractical become practical and it's worth a reexamination on that basis alone.

Paul Egerman – Software Entrepreneur
Yes, I agree with that. I think if it gets rolled out and it's successful it probably then should be the standard for everything else.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think that's a long discussion. I don't want to have to pin what I'm saying now on that—

Paul Egerman – Software Entrepreneur
....

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But it doesn't require certificates. It just requires two factors, and one of them can be metrics, which is not PKI. But I wanted to bring up another angle is that if we look at the three largest federal agencies that private industry will be exchanging information with, the VA, CMS, and DoD all require two factor authentication for this kind of remote access, some of them for reasons, direct access. I know I heard that people want to be able to do single sign-on across multiple organizations, so if they use … or something to exchange authentication information, I'm wondering what those agencies will require for somebody to really exchange information with them through a single sign-on type thing. Is that going to force level three type authentication?

Deven McGraw – Center for Democracy & Technology – Director
I don't think we know enough to say that, Dixie.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It is certainly a concern. We had many discussions, this is David, in the Direct Connect best practice debate about if you want to share trust circles with a federal bridge you have to meet their standards.

Deven McGraw – Center for Democracy & Technology – Director
Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Which for people who want to communicate with the VA directly is going to be a problem.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Although I think what Paul says makes a lot of sense. I do keep thinking that they're unambiguous in the message, the public at large is unambiguous with the message that they want to be told what to do and they will do it, and they want to just keep it easy for us to do, don't make us do a lot of analysis.

Deven McGraw – Center for Democracy & Technology – Director
With all due respect to the people who are making those claims, and I certainly understand where they're coming from, having been a private practice lawyer for many years, and the uncertainties and the gray areas and the flexibility that is currently allowed in the law is problematic. Certainty gives you more to hang your hat on. But having said that, I've also heard that when you're certain and you set the bar pretty high, that's problematic as well. When you don't allow flexibility for different use cases, that's problematic. When you set one standard that works for well-resourced institutions and doesn't work so well for rural healthcare providers, that's problematic as well. I think the best we're going to be able to do is to get more guidance out there that is both by use case as well as, or maybe even organizational size that can be helpful for people to use. Whether that's sort of maybe even a development of Safe Harbors that people can rely on more from a legal standpoint. But I, number one, don't think we have enough expertise on this group to do really specific examples that are going to stand the test of time and work across multiple organizations. I think there's just too much fluidity in the different scenarios out there.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, I don't think this is setting the bar too high at all. I think we should remain in lockstep with what DEA is referring. That's my vote.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So just to make sure I understand, your suggestion is that every provider that ever calls in from home to look up a result should, granted it's two parts, one, should use the authentication level required by DEA for prescribing controlled substances. The second part I think you'll say no to is, they should do it for each result as they do for each prescription now.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

No, I think it should be a one-time log-in, but I do think for that one-time log-in to do what you need to do, I think that what the DEA is requiring is not overly burdensome. As we've discussed previously, the banks are doing it for their banking right now. This is not overly burdensome.

Paul Egerman – Software Entrepreneur
Dixie, listening to what you're saying—

M
... wrong, right?

Paul Egerman – Software Entrepreneur
My question or concern is why isn't the DEA stuff being used a lot?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Because it's a new regulation.

M
It's a new reg that hasn't been rolled out. Everybody has to change their software pretty dramatically to make it work with the DEA reg, which is another point to consider actually.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
But that's almost a side issue, because they are going to specific transactions. They are going to using the same level of security for operator functions that change levels of security, as they do for prescribing. I guess I'm flummoxed by this statement that this is the second level that banks are using.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's not. It's not the same.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
They're doing two factor, but it's not the strength that DEA requires.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I'm like Paul. I think given the lack of experience with DEA impact on provider productivity and software industry surrounding that, which we will gain in the next couple of years, and given the fact that this is a rapidly advancing area where devices are still being invented, particularly around biometrics, cameras on the computer can now be used for biometrics and things that nobody dreamed of a few years ago. That it's like Paul said, it's got to be more than level two, but we don't say much more than that. It's got to be multi-factor more than level two.

Deven McGraw – Center for Democracy & Technology – Director
Right.

M
I'd like to just add the comment that two things that you know is not two factor.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, I think you flesh out—

M
Well, you know here's my password and my ... in Edwardsville, and most people that I think of when they hear the phrase "two factor authentication" they think something you know, something you are, or something you have, pick two. Two things that you know, even if they're in the form of challenge

questions aren't—they have alternate spellings for the city where I went to high school, so I've got some of my challenge questions written down.

Deven McGraw – Center for Democracy & Technology – Director
Yes, on a yellow sticky beside your computer.

Paul Egerman – Software Entrepreneur
That's right. Even the defaults are too fast, which is something you have. So if you look at the vendor example that was discussed, if you lose your cell phone then whoever's got it has one of the two factors, because it's got a cell phone with whatever certificate on it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
They have one. They don't have the other one.

Paul Egerman – Software Entrepreneur
They don't have—

M
Yes.

Paul Egerman – Software Entrepreneur
So the same is true of if you write down what was the name of the elementary school you went to and you paste it on the back of your cell phone.

M
The good news is that yellow stickies tend to fall off cell phones, but the principle's fine.

Paul Egerman – Software Entrepreneur
Yes.

Leslie Francis – NCVHS – Co-Chair
Just a comment about what you said a couple of minutes ago. I don't know, if I was an organization I don't know how I would understand it's got to be more than two. I think a different way to do it would be to say, I favored what Dixie was suggesting and why not just say it needs to be either NIST level three or the organization needs to propose something that by analysis shows as secure.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Then we're back to do we set up an agency with a budget to pre-approve these or do they just wait until they're at risk for millions of dollars and then find out whether they have the police agree with them.

Leslie Francis – NCVHS – Co-Chair
Well, they have a Safe Harbor, though, if you do it that way.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What she's suggesting is exactly the same as what HIPAA does with their addressable—

Leslie Francis – NCVHS – Co-Chair
Exactly.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
—patient stacks.

Paul Egerman – Software Entrepreneur
Well, maybe a variation of what you're saying, Leslie, would be that what we could do is to say level three is the best practice and that people have to do this risk analysis, so if they want to do less because of utilities it has to be based on some evaluation.

Leslie Francis – NCVHS – Co-Chair
Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This one will be a challenge for the certification process.

Judy Faulkner – Epic Systems – Founder
Yes, I'd be careful of the words "best practice."

Paul Egerman – Software Entrepreneur
It may be best practice and you don't test or certify around it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is not certification. Certification is products. The Standards Committee will have to address what's required for certification. What we're talking about here is policy that would be in HIPAA.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Virtually every vendor probably has no trouble implementing the NIST recommendations now because they have a catalog of different authentication processes that can be applied and they can set up the product to be tested for. On the other hand, site certification for a hospital would probably get closer to what we're talking about here. I like the approach that we set a level, leave some room for evaluation, and that periodically ONC goes back and revisits this issue, because it is rapidly changing. And even if we try to create flexibility we're still likely to find that our flexible formula either fell into the trap of plausible deniability or is unnecessarily low based on the current level of rollout of infrastructure and so forth.

Paul Egerman – Software Entrepreneur
Leslie's suggestion is, if I understand it right, instead of saying it's got to be better than two, Leslie's saying it really ought to be three, but there are some reasons why you can do less than three if you want.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I really like Leslie's approach because it capitalizes on what's already in regulations and could easily be incorporated into HIPAA as an addressable implementation spec. So I like that approach.

Deven McGraw – Center for Democracy & Technology – Director
Right, but let me make sure I understand what you mean by it's got to be three. We're driving to a level three of assurance and in terms of the factors that are involved if you cannot meet the level three that is in NIST and you have reason for not doing that, you're documenting it. So level three would be akin, as Dixie said, to an addressable spec under the security rule meaning if you choose not to do the multi-factor authentication using something you know and something you have, then you have to document that.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Just to clarify, though, if level three was made something analogous to an addressable specification, it is in no way optional. It would mean that you're required to do level three if it is reasonable and appropriate based on factors such as your resources, the sensitivity of the information, and it's only if you can document that as not reasonable and appropriate then you have to do an alternative equivalent measure.

So I don't want people to have the impression that you have the option of saying that I'm not going to do level three if it's addressable.

Paul Egerman – Software Entrepreneur
What do you think, Adam, about making it a little less than what you just said, making this best practice or guidance or saying that we're waiting to see how the market accepts the DEA recommendations and here's our guidance, is to do level three unless you have some risk analysis that says you don't need to.

Judy Faulkner – Epic Systems – Founder
Should we do level three when it's more than one patient they're looking at? In other words, if you're just looking at one patient you have a limited amount of danger you can do.

Deven McGraw – Center for Democracy & Technology – Director
It depends on what you're looking at in that patient's record.

Judy Faulkner – Epic Systems – Founder
Well, yes, and the situations would probably be that the patient is a VIP of some sort or the patient's a relative. Other than that, if you're doing it for advertising then you need to be looking at lots of patients.

M
But the distinction between one patient and multiple patients can be pretty slippery given your access in an application.

Judy Faulkner – Epic Systems – Founder
Well, yes, but that could be figured out, I think. In other words, just like you were saying earlier about balancing the amount of the transaction in banking with the level of security, should we be slowing down the person who's trying to find out whether this child needs to go to the emergency room right away or no by multiple levels. Versus I want to look at a whole bunch of stuff or I want to look at President Obama's information, you know something—

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Just to add to that, though, it may not be a VIP. It's not uncommon for us to deal with someone looking up an ex-spouse for purposes of a custody hearing.

Judy Faulkner – Epic Systems – Founder
Yes, that's what I was saying. That's the third situation, that's a relative. Then some of those questions if it's a relative are almost meaningless because they know the answer anyway.

Deven McGraw – Center for Democracy & Technology – Director
But those are not decisions that to me get resolved at a national policy level.

W
Exactly.

Deven McGraw – Center for Democracy & Technology – Director
I just feel like where there seem to be two differences of opinion on the tiger team, it is do we set the threshold as level three with multi-factor authentication according to NIST unless you can come up with a good reason why you can't get there, versus where we started. Which is that we want a high degree of confidence level that matches three but we don't think that the authentication factors that would be required today under the NIST framework to get you there are necessarily doable today, but we want people to do more than two factors or more than one factor really. We didn't say people should do more than two factors.

Paul Egerman – Software Entrepreneur
Deven, I like—

Deven McGraw – Center for Democracy & Technology – Director
We want to study what's happening with the application of the DEA approach and others that are of higher level.

Paul Egerman – Software Entrepreneur
It sounds like the DEA even compromised on level three, right?

Deven McGraw – Center for Democracy & Technology – Director
They compromised on level four and then allowed biometrics.

W
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That level three in the NIST document disallowed biometrics, so they compromise on three.

Deven McGraw – Center for Democracy & Technology – Director
I thought that where the DEA started initially was at level four.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Maybe so.

Deven McGraw – Center for Democracy & Technology – Director
In terms of the level of assurance.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Level three in NIST disallowed biometric, and which I have here on the slide.

Deven McGraw – Center for Democracy & Technology – Director
No, that's absolutely accurate. I was just saying that's not exactly where they started. They started even higher than that.

Paul Egerman – Software Entrepreneur
Let me just take the direction to different levels, I'm also looking at the cost. If I hear it right, and I'm not sure I'm hearing this right, but there's three alternatives on the table. The first one is something that says more than two and gives examples. The second alternative is to say three, and there's a variation of that three or it might be to say DEA style three, but that's the second one. The third one is, if I understood, Leslie suggested it, is three with some wiggle room.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes, and if we talk about wiggle room—

Paul Egerman – Software Entrepreneur
Are those the three choices we have?

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Okay.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If we talk about wiggle room, do we talk about break the glass conditions to deal with Judy's—

Deven McGraw – Center for Democracy & Technology – Director
I think the wiggle room is your risk assessment of use cases within your own institution.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So let me back up, I'm worried about Judy's use case. I think it has a significant reality issue so even more it's going to be a continual source of discussion. I'm trying to think whether there's a formulation that can be apply to break the glass here, and I'm not, to be honest.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that that's a different requirement entirely. I think that we're talking about basic authentications, period.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If you can't do anything else until you're authenticated, then there's no special allowance for breaking the glass.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Even in HIPAA, that's a separate requirement.

Paul Egerman – Software Entrepreneur
Deven, looking at the clock, I think we've had a good discussion. What should we do with these three choices? Should we do a vote?

Deven McGraw – Center for Democracy & Technology – Director
No, I don't because we've never operated that way.

Paul Egerman – Software Entrepreneur
Okay.

Deven McGraw – Center for Democracy & Technology – Director
We have a Policy Committee meeting on Wednesday and I think that we have a discussion with the Policy Committee and get their input on some of these options before we finalize, is what I suggest we do.

Paul Egerman – Software Entrepreneur
But one of the things, though, Adam's comment, the previous one was helpful to me because that's how we lose the forest for the trees. So the issue is just when we make this decision how is it enforced? Is this going to be a regulation? Is this going to be a specification? Is this going to be, as—

Deven McGraw – Center for Democracy & Technology – Director
How is any of our stuff enforced?

Paul Egerman – Software Entrepreneur

Yes. What's going to happen to it? Is it just going to be guidance so when people ask the question that Dixie talks about, tell us what to do, at least there's an answer?

Deven McGraw – Center for Democracy & Technology – Director
Our recommendations go to the Policy Committee, and whatever gets endorsed from the Policy Committee goes to ONC. It has policy levers at its disposal, to the extent that it's part of HHS and there are other agencies within HHS, like OCR, where that has jurisdiction over HIPAA. If they find it appealing, we actually don't get to necessarily decide that stuff, although we have in some cases been very specific about policy levers that we want to see used, but that's not a decision that we get to make. In discussions that I've had, certainly with staff at ONC, there's a great desire to take the recommendations that we've been generating and fold them potentially into the conditions of trust and interoperability that are part of the NHIN or NW-HIN, or whatever we're calling it these days, the Nationwide Health Information Network, the brand.

Paul Egerman – Software Entrepreneur
That's helpful. I have to say as I listen to all of this, even though I was the one that suggested more than two, the idea of three with some flexibility sounds appealing.

Judy Faulkner – Epic Systems – Founder
I'm confused about one thing. It was said, I think by Dixie, that you don't have to do this each time. How do you not do it each time? Maybe I'm misunderstanding something very basic here.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What he was saying was each query, like if you authenticated to the EHR and you were allowed access to the EHR and you accessed David McCallie's record, then if you wanted to access Deven McGraw's you'd have to authenticate again. What I was saying is that no, if you want to get access to the EHR you can just—

Judy Faulkner – Epic Systems – Founder
Ah, so it's each time. What I'm thinking of, because I'm married to a pediatrician who's on call for emergencies at night, is sometimes it's very quick and it's get your kid into the ED right now and I'll meet you there. How do you get that information quickly? That was where I'm coming from. But in that situation that's an each time, because they're not on all night long. They're on sporadically.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Without access to an EHR, that's a communication tool that's—

Judy Faulkner – Epic Systems – Founder
Yes, but it would be much better with access to an EHR, and that's what you want.

Paul Egerman – Software Entrepreneur
Yes. Let me see if I've got this right. In your case the pediatrician might have a home computer or a laptop—

Judy Faulkner – Epic Systems – Founder
Absolutely.

Paul Egerman – Software Entrepreneur
—and the home computer or laptop probably has a digital certificate on it, it's doing level three, so your spouse then simply signs on to the computer how they normally do it, it's user name and password. It's not a big deal.

Judy Faulkner – Epic Systems – Founder
Do you think that would be all in that circumstance?

Paul Egerman – Software Entrepreneur
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, because there are two factors.

Paul Egerman – Software Entrepreneur
There are two factors, and the one factor was that there was already a certificate on that laptop.

Deven McGraw – Center for Democracy & Technology – Director
But I thought we said that the computer didn't count.

Judy Faulkner – Epic Systems – Founder
That's what I thought too.

M
Yes, me too.

W
The computer doesn't count, Paul.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What we're saying is that the IP address of the computer doesn't count. But if the computer has a digital certificate for that individual that is a second factor.

Paul Egerman – Software Entrepreneur
So what happened there was your spouse under level three at some point already had a digital certificate and one time had to do something, had to authenticate themselves and answer a bunch of questions, do something, and then a certificate was somehow installed on that laptop and now they're good to go.

Judy Faulkner – Epic Systems – Founder
Okay.

Deven McGraw – Center for Democracy & Technology – Director
Again, I actually think what I'm hearing is that people do want more than two factors. Where we are breaking down is whether there would be a requirement to do the multi-factor authentication levels a la the NIST framework, which is much more prescriptive, about the particular categories that these factors need to be in and what's useful or not. Whether that's required or whether it's preferred but with some wiggle room, or whether in fact we want to set what is required as more than just a single factor but allow entities to, through risk analysis, determine how they navigate that based on use case scenario. But again with the common denominator being more than just single factor.

Paul Egerman – Software Entrepreneur
Just to clarify, at one point you said more than two factors, but what you really mean is at least two factors, right?

Deven McGraw – Center for Democracy & Technology – Director

Two, that's right. It's sort of morphed into more than two and I think people were mixing up the discussion of level of assurance versus the number of factors.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I think you need something to take to the meeting on Wednesday of next week. I'm not prepared to vote because I'm still confused on some of these options, but the general statement of more than user name and password and probably involving something you have rather than just something you know, I think I could get into.

Paul Egerman – Software Entrepreneur
Yes, but doesn't that put you at level three.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Once you said "something you have," I think we're at level three.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

M
I think the question is something you can get, like a one-time password or something. It's not technically something you have.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think what he said is on option two right now.

Paul Egerman – Software Entrepreneur
Yes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
If you have a device that will get you to a one-time password, I would say that's something you have. If you can call the help desk and get a one-time password, I'm not sure what that is, but if I was running a hospital that had pediatricians on my call I'd sure have that available as an option.

Deven McGraw – Center for Democracy & Technology – Director
Yes, that's a hard token. That's something you know.

M
I think that, Wes, you rendered that as your opinion.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes.

M
That's the problem with the NIST document, it removes those opinions and that's why DEA compromised and why we're nervous, I think, saying it's just simply NIST level three assurance. It's too prescriptive.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst

I'm a little behind in this last week's call, but I think we all agree that user name and password is inadequate, we certainly would want the Policy Committee to either endorse that or send us back to the drawing board, and that there is a complex trade-off between what constitutes more. And we'd like to have a little bit more time to work on that, and then we can take some more time to work on it.

Deven McGraw – Center for Democracy & Technology – Director
I think that's right. We have an opportunity to get some early feedback from the Policy Committee before we're done—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Right.

Deven McGraw – Center for Democracy & Technology – Director
Usually we present them with what we think is the best way to go and we've batted some out of the park using that approach but we, on more than one occasion, have gotten sent back to reconsider some issues that we hadn't thought of.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I would like to see you also present to them the option that Leslie suggested.

Deven McGraw – Center for Democracy & Technology – Director
Absolutely. But to have a general discussion with them versus asking them to endorse a specific outcome, because we haven't really coalesced around one.

Paul Egerman – Software Entrepreneur
So it's sort of like how prescriptive should we be in the issue. The other issue is to what extent should we be concerned that we're specifying something on a broad national scale that isn't in use in a significant way right now. So those would be the two issues.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Leslie Francis – NCVHS – Co-Chair
What I was trying to capture, maybe slightly inartfully, but I think it should be a high level but not prescriptive. Do you see what I'm saying?

M
Yes.

Leslie Francis – NCVHS – Co-Chair
The disadvantages of saying you've got to do it this way are obvious.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Yes.

Leslie Francis – NCVHS – Co-Chair

On the other hand, particularly in a context in which it's not easy to distinguish between whether you're accessing one patient or a bunch, risk levels and so on, because with banks I only get my own information. I never get other peoples.

Paul Egerman – Software Entrepreneur
These are great comments. An excellent comment, Leslie. The observation I had, as I'm looking at my clock, is we don't know, there may be a member of the public who if they're making a comment I'm sure will have an excellent comment also, so should we just open ourselves for public comment? Deven, do you have something else you'd like to say?

Deven McGraw – Center for Democracy & Technology – Director
No, again the charges we'll get some feedback from the Policy Committee and on our next call we'll see how much further we can take this in terms of actual consensus. I do think we should open it up to the public.

Paul Egerman – Software Entrepreneur
Yes, I think so. The one comment, I just want to thank everybody, excellent discussion, really interesting issues. The one comment I'd also give is that as you think through our next call is to think how this recommendation might change, we've got, instead of EHR users we get to patients and consumers. So, having made that comment, Judy, why don't we open ourselves for public comment.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Operator, can you check and see whether anybody wishes to make a comment, please? Deven and Paul, the next call is on March 7th, right?

Paul Egerman – Software Entrepreneur
That's correct.

Deven McGraw – Center for Democracy & Technology – Director
That's correct.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay, just a reminder.

Deven McGraw – Center for Democracy & Technology – Director
Thank you.

Paul Egerman – Software Entrepreneur
Thank you. I appreciate that. Does the silence mean we don't have any public comments?

Judy Sparrow – Office of the National Coordinator – Executive Director
It sounds like it.

Operator
Yes, we do not have any callers at this time.

Paul Egerman – Software Entrepreneur
Great. So let me just take a minute to thank you, Judy Sparrow, for all your help in organizing the meetings, and thank the members of the tiger team for an excellent discussion. Hopefully, we can try to wrap things up on March 7th, because what we'd like to do is also consider the issues of public access or consumer access, and the consumer access also will be a different environment because patients will be

looking at presumably a patient portal with somewhat limited different capabilities. But that's also just a general comment to put in the back of our heads. Thank you very much.

Anything else you want to add, Deven?

Deven McGraw – Center for Democracy & Technology – Director
No, thank you, Paul. Thank you, tiger team. Thank you, staff. It's much appreciated.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you.

Paul Egerman – Software Entrepreneur
Yes. Take care, bye-bye.

Public Comment Received During the Meeting

1. What about the use-case --- HIGHLY authenticated Organization (TLS - mutual authenticated certificates) with a low LOI on the user - but a declaration of Emergency Access (Break Glass) that indicates life-or-limb is in danger.

2. Federation is a wonderful thing -- Original organization that has employed individual is fully responsible for LOI, federation allows others to 'trust' them... responsibility is a chain from the trusting party all the way back to the original organization... original organization is responsible.

3. YET the risk of NOT providing healthcare (denial of service) is also VERY different than banking... don't provide banking and someone is without money, don't provide healthcare and someone gets sicker, more pain, or worse.

4. Once the individual has logged on remotely to the institutional portal that gives access to the EHR and network query capability, consider the role based access limitations at the institutional level as a surrogate for one of the factors, assuming the entity's system would not permit access to the network through an EHR and/or e-health information network to anyone but authorized users.

5. Unstated Assumptions are NOT HELPFUL

6. Place risk on the one CLAIMING the identity, not on the one RELYING on it.

7. With PHYSICAL devices, the expectation is that one KNOWS when they loose it.... and thus the use of the PHYSICAL device gets REVOKED as authentic

8. Isn't a cellular phone often used as if it is a physical token? Isn't a cellular phone - smart phone - a computer? So, why are you so quick to say that there is NO POSSIBLE WAY for a computer to be a token

9. Seems the suggestion being discussed would DISALLOW any iPad use.... given HIMSS observation this would not be acceptable.

10. NHIN Exchange is OPENLY DOCUMENTED -- see Authorization Framework at http://exchange-specifications.wikispaces.com/Authorization+Framework+Page+1

11. NHIN Exchange supports SAML federation for user identity in addition to system-to-system authentication (TLS)

12. Federation allows on a transaction-by-transaction basis what LOI was used (along with Purpose of Use, Role, Context, etc). Allowing policy to be flexible and to change over time.